WLCG SOC WG Workshop

David Crooks
Liviu Vâlsan

Introduction

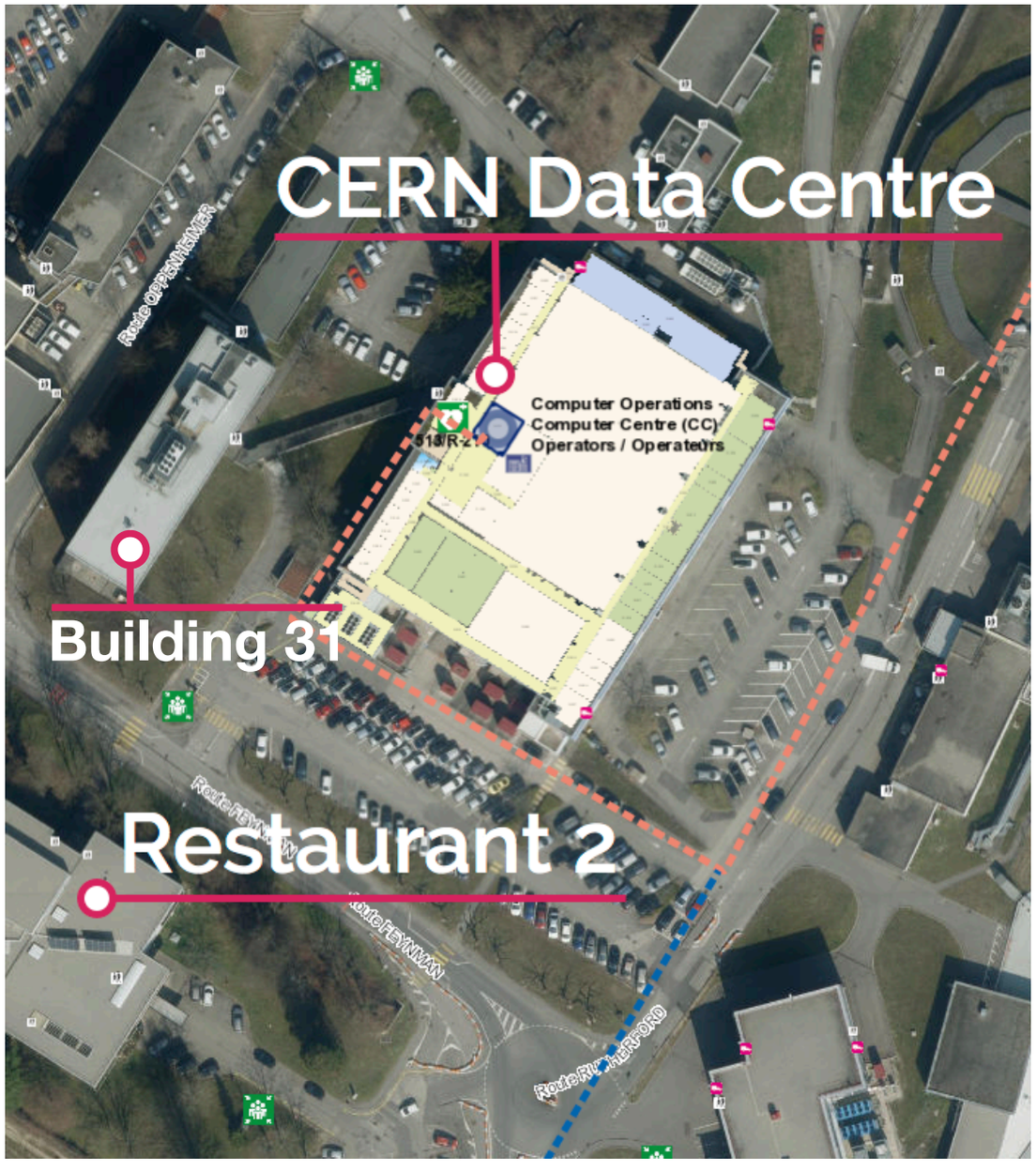
- Welcome to the first WLCG SOC Workshop / Hackathon!
- 27 registered attendees (inc. Liviu and David)
  - 17 in person
  - 10 remote
  - 19 institutes
  - 8 countries
  - Most for both days
- Very happy to see everyone

WLCG
Worldwide LHC Computing Grid

Logistics

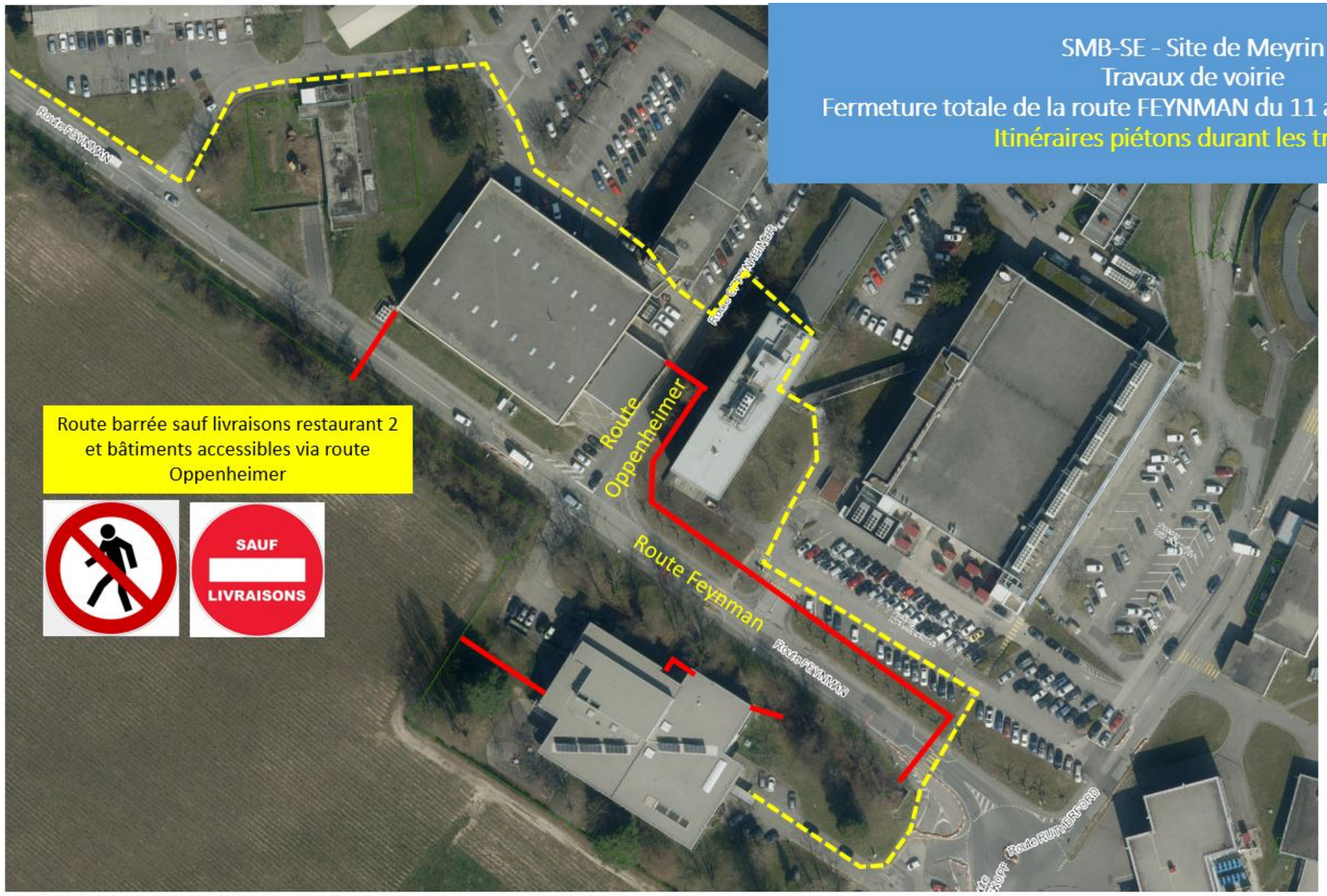
- Rooms:
  - Monday: 513 / R - 070
  - Tuesday: 31 / S - 028
- Location of restaurant & coffee
  - R2

Logistics



WLCG
Worldwide LHC Computing Grid

Logistics / Road works



WLCG
Worldwide LHC Computing Grid

WiFi network access

- Eduroam available everywhere on the CERN site.

- If you do not have Eduroam access, you will need to register at https://landb.cern.ch/landb/selfregistration/

- After registration (and some manual validation), you will be able to connect to the “CERN” WiFi SSID.

WLCG
Worldwide LHC Computing Grid

Logistics

- Fire information
- If the fire alarm rings, evacuate through nearby exit
- Assembly point is parking area between buildings 513 and 31

Logistics

- Timings are flexible
- Have the room today until 6 pm
- Tomorrow planned to start at 9 am if everyone is OK
  - Understand that’s early for sites for the UK
  - Coffee & croissants in the morning
  - Other coffee breaks in R2

Plan for the workshop

- Today
  - Introduction (what we're doing now)
  - Discussion of site goals & outcomes
  - CERN SOC demo
  - Structure for tomorrow
  - Dinner if there's interest

WLCG
Worldwide LHC Computing Grid

Plan for the workshop

- Dinner options
  - Pizza: Meyrin
  - Café de l’Aviation: Blandonnet
- Perhaps meeting there at 7pm

Plan for the workshop

- Tomorrow
  - Installation of components
  - Integration
  - Documentation
  - Provisioning
  - Areas of interest

WLCG
Worldwide LHC Computing Grid

Plan for the workshop

- Wrap up
  - What we've achieved
  - Feedback
  - Plans for next time
  - Activities for the working group
  - Continue discussions in R1 depending on travel…

WLCG
Worldwide LHC Computing Grid

Background

- SOC and (then) Traceability and Isolation Working Groups, came from Cloud Traceability TF

  - Identify need to monitor cluster environment in a new context which can include virtualised / containerised systems

  - Potentially more opaque than existing grid systems

  - Network monitoring key to understanding cluster state

Security Operations Center

- The purpose of a Security Operations Center (SOC):
  - Gather relevant security monitoring data from different sources
  - Aggregate, enrich and analyse that data for use in the detection of security events and any subsequent actions
- A SOC consists of a set of software tools and the processes connecting them

WLCG
Worldwide LHC Computing Grid

Metron (OpenSOC)

- Developed by CISCO, OpenSOC part of initial impetus for this work
- Due to acquisitions by CISCO, OpenSOC moved to closed source
- Open source project moved to Apache, renamed as Metron
- Initially in incubation; left that stage earlier this year
- Currently of interest to us as a reference

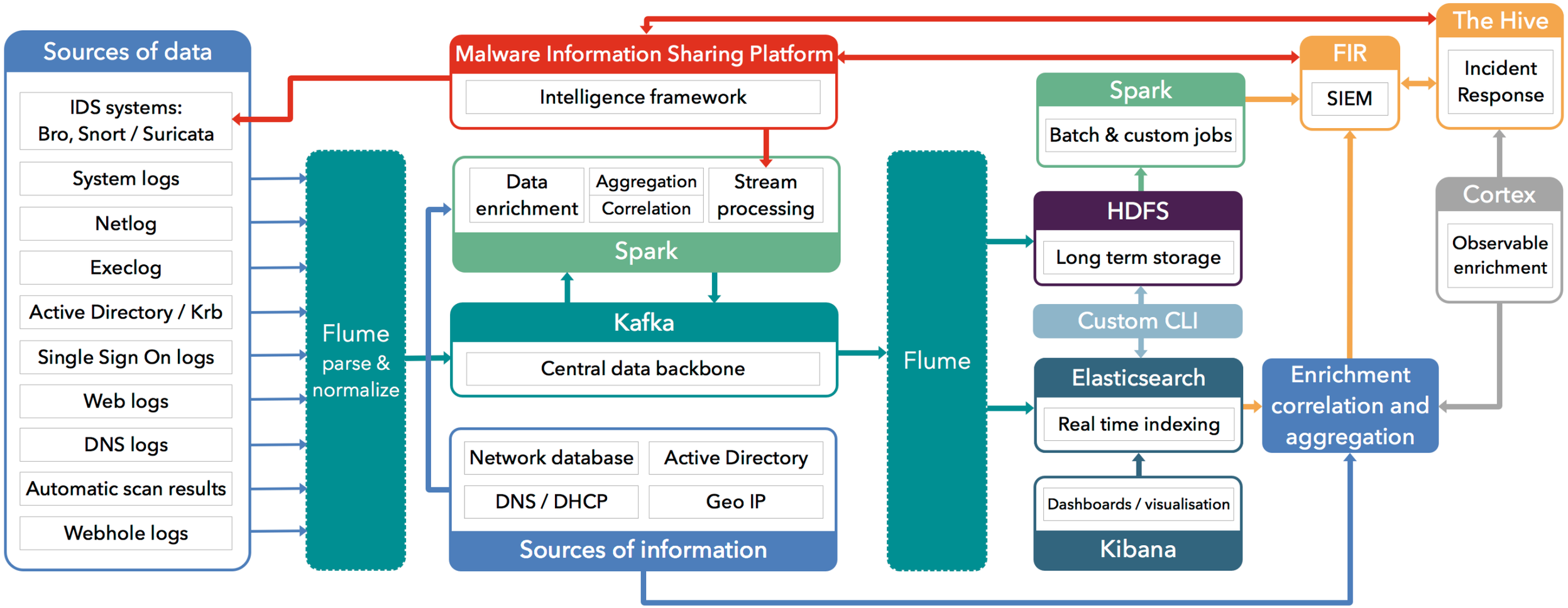
WLCG
Worldwide LHC Computing Grid

CERN SOC

- Closely following and benefitting from work on the CERN SOC
- Mostly leave to the demo later by Liviu, but call out some points
- Common features:
  - Data ingestion
  - Data analytics
  - Data storage (short term and long term)

WLCG
Worldwide LHC Computing Grid

CERN SOC



WLCG
Worldwide LHC Computing Grid

Two questions

1. What is happening in my cluster?

2. What events are taking place that we need to care about? (internally or externally)

Two questions

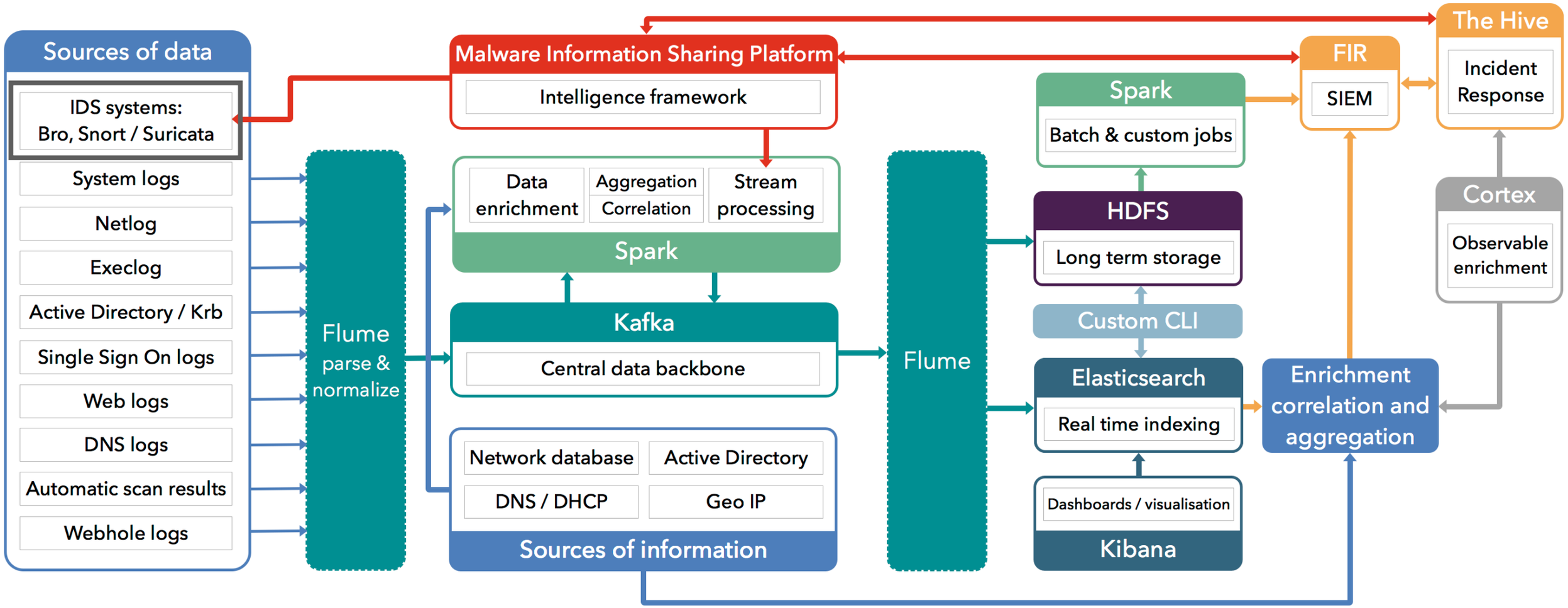
1. **What is happening in my cluster?**

2. What events are taking place that we need to care about? (internally or externally)

Network Monitoring

- IDS: Bro
- Wide use in the US
  - 100 Gbps setup at Berkeley Lab
    - https://commons.lbl.gov/display/cpp/100G+Intrusion+Detection
- Flexible & Scalable
  - Configure as single node or cluster

CERN SOC



WLCG
Worldwide LHC Computing Grid

Network Monitoring

- Recommended Baseline Requirements
  - System type: Hardware
  - Number of cores: The recommendation is to have at least 12 physical cores. Rule of thumb is that one core is able to handle 800 Mbps - 1 Gbps of network traffic
  - Memory: At least 64 GB. Each Bro worker requires on average 6 GB of RAM
  - Disk space: As much as you can afford

WLCG
Worldwide LHC Computing Grid

Network Monitoring

- Workshop outcomes
  - Hoping to see results from different configurations in a grid context
  - Explore what data / storage rates people see
  - *Longer term*
    - What output do we consider useful?
    - Are there different useful levels of service?

WLCG
Worldwide LHC Computing Grid

Two questions

1. What is happening in my cluster?

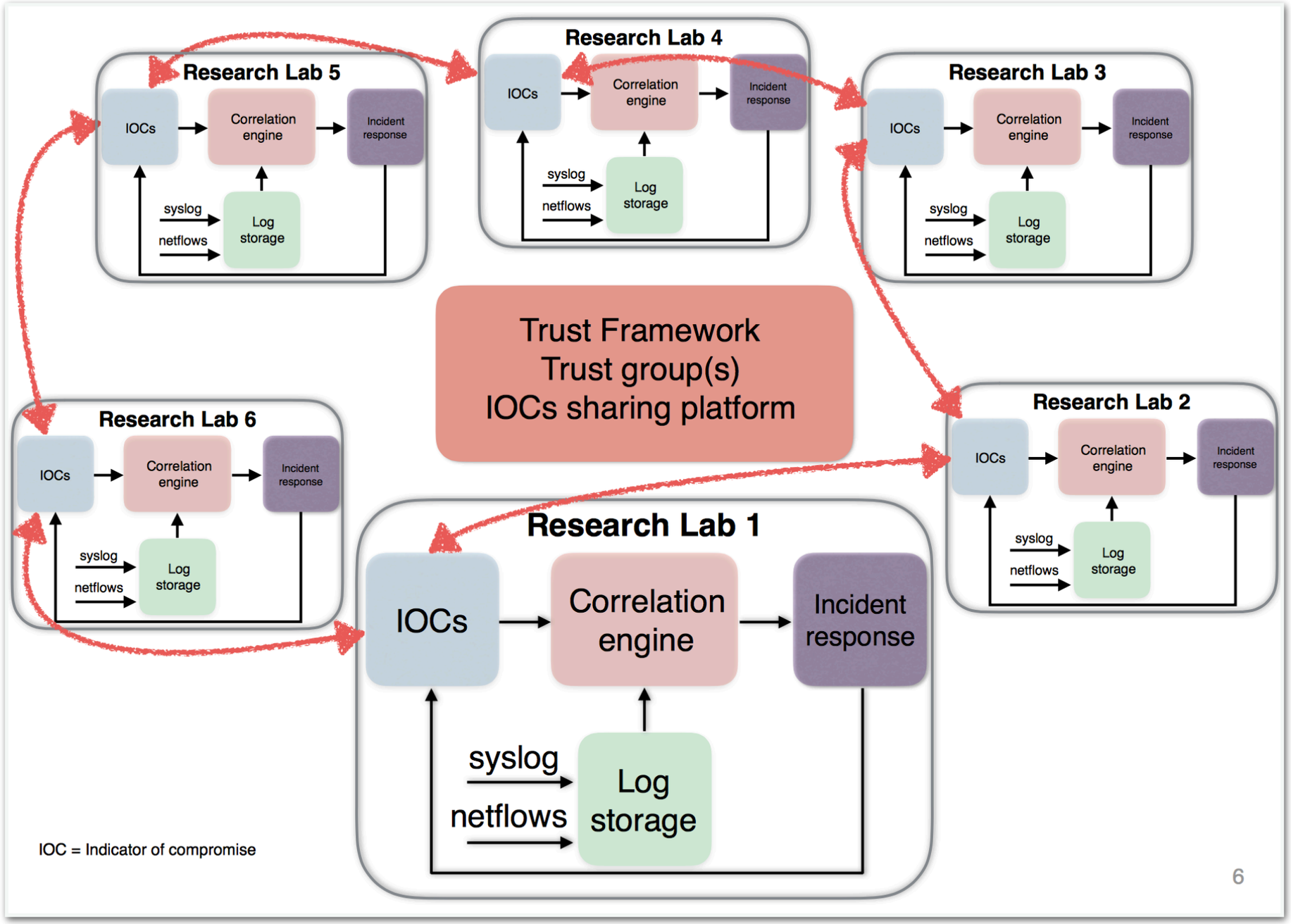
2. **What events are taking place that we need to care about? (internally or externally)**

Threat Intelligence

- Second major strand of the working group
- The future of academic security (Romain)
- http://indico.cern.ch/event/505613/contributions/2227689/attachments/1349009/2047093/Oral-109.pdf

WLCG
Worldwide LHC Computing Grid

Threat Intelligence



WLCG
Worldwide LHC Computing Grid

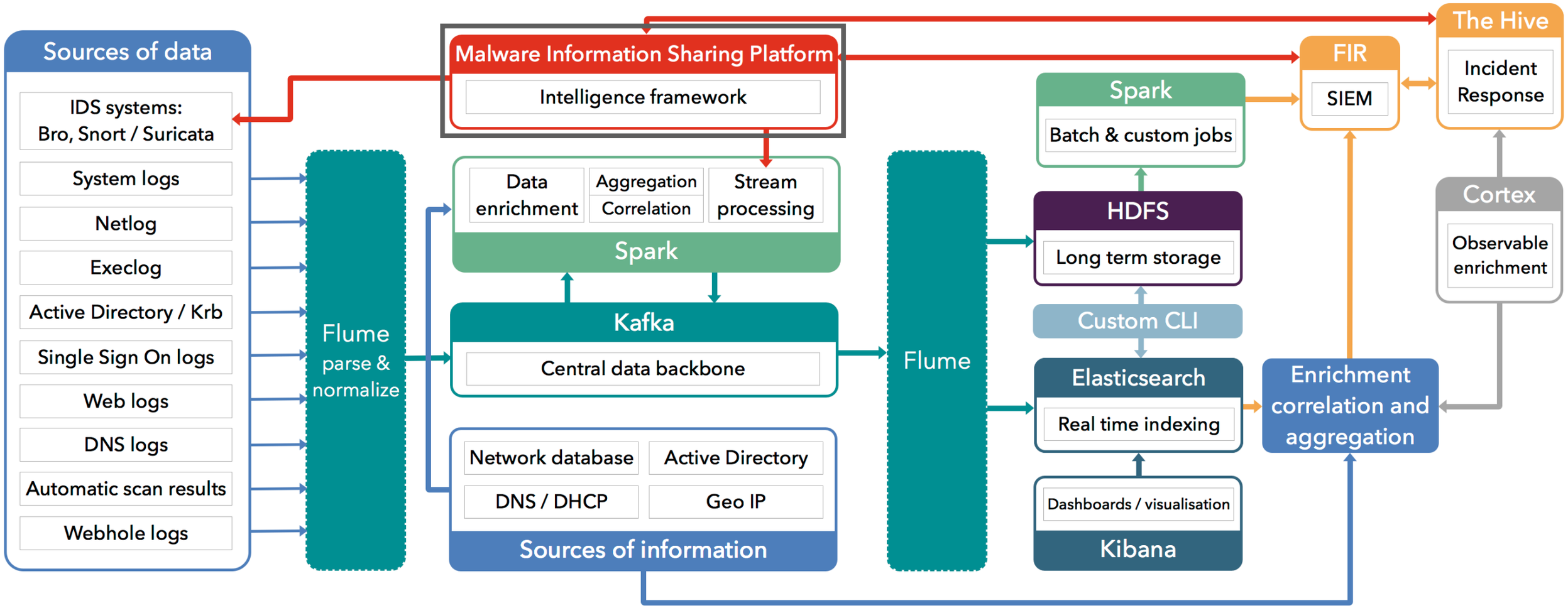
Threat Intelligence

- Common response
- Shared responsibility
- Fundamentally collaborative
  - In particular, one goal of this group is to explore collaboration between grid and institute / campus security team

MISP

- Malware Information Sharing Platform
- *“A platform for sharing, storing and correlating Indicators of Compromises of targeted attacks. Not only to store, share, collaborate on malware, but also to use the IOCs to detect and prevent attacks.”*
- Allows development of trust frameworks between sites to allow rapid sharing of threat intelligence
- misp-project.org

CERN SOC



WLCG
Worldwide LHC Computing Grid

Threat Intelligence

- Recommended Baseline Requirements
  - System type: VM (or a container)
  - Number of cores: 2 cores
  - Memory: 4 GB of RAM
  - Disk space: 10 GB

Threat Intelligence

- Workshop outcomes
  - Deploy MISP web app and test sync to WLCG instance
  - Explore MISP API
  - Integration with Bro
  - *Longer term*
    - Cultural shift in intelligence sharing

WLCG
Worldwide LHC Computing Grid

Initial model

- Build the full SOC model over time; start with key components
- Network monitoring
  - Intrusion Detection System (IDS)
  - Bro
- Threat Intelligence
  - Malware Information Sharing Platform (MISP)

WLCG
Worldwide LHC Computing Grid

Two strands

1. Technology stack (this workshop!)

2. Social and political cultural shift in sharing of intelligence

WLCG
Worldwide LHC Computing Grid

Working Group

- In that context, WG looking to build stack appropriate for different sites

- Alongside, consider way of working to best incorporate these components

WLCG
Worldwide LHC Computing Grid

Roadmap [now]

- Basic components now
- Bro: active monitoring
- MISP: threat intelligence
- Follow CERN, OSS

WLCG
Worldwide LHC Computing Grid

Roadmap [next]

- Next steps:
  - Advanced alerting / notification
  - Ingest Bro data to Elasticsearch
  - Real time processing
  - Distributed storage
  - Other sources of data
  - Other tools
  - Other integrations

WLCG
Worldwide LHC Computing Grid

Important questions

- Once a security incident is detected how can we get the full picture of the incident (when exactly it started, what's the extent of the incident, etc)?

Important questions

- Important questions which need answers through this work (not just today!)
  - What data do we need?
  - What *sources* of data do we need (intersection with traceability)
    - Where / how to tap network?
    - How to handle data sharing / protection for different user groups
    - How to consider different contexts:
      - Institution / NGI / WLCG / Other
- Critical to include sites of different type in this work

WLCG
Worldwide LHC Computing Grid

Goals for today

- Establish individual site goals
  - For example: Full stack, individual components, provisioning, documentation, integrations, other areas of interest…
- Make sure that baseline requirements are handled
  - Nodes, network taps, etc…
- Establish structure for Tuesday

Questions + contact

- wlcg-soc-wg-workshop-dec-2017@cern.ch should contact everyone registered for the meeting

- Propose to merge this into main wlcg-soc-wg group afterwards if everyone is happy to do so

- Contact through the workshop:
  - liviu.valsan@cern.ch
  - david.crooks@cern.ch

WLCG
Worldwide LHC Computing Grid